UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

OLIVIA FRAGOMENI, individually and on behalf of all others similarly situated, Plaintiff, v. DAVID'S BRIDAL, INC., Defendant.	Case No. **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Olivia Fragomeni ("Plaintiff"), on behalf of herself and all others similarly situated ("Class Members"), alleges the following against Defendant David's Bridal, Inc. ("Defendant"), upon Plaintiff's knowledge and information and belief, including the investigation of counsel.

DAVID'S BRIDAL SUFFERED A MASSIVE DATA BREACH

1. This action arises from Defendant's failure to safeguard Plaintiff's personally identifiable information ("PII") and the proposed Class Members, thousands of Defendant's current and former employees and customers. Specifically, on or about January 22, 2024, the notorious criminal ransomware group known as LockBit 3.0 ("LockBit") accessed Defendant's network systems and exfiltrated Plaintiff's and Class Members' PII stored therein, including, upon information and belief, their names, dates of birth, Social Security numbers, identification documents, employment information, and tax information, causing widespread injury and damages to Plaintiff and Class Members.

2. Instead of remedying its deficient cybersecurity practices following LockBit's

theft of Plaintiff's and Class Members' PII from its systems, Defendant did nothing. As a result, *another* notorious criminal ransomware group known as WereWolves hacked Defendant's network and obtained Plaintiff's and Class Members' PII on or about February 14, 2024—*less than one month* after LockBit did the same (LockBit and WereWolves breaches collectively, "Data Breach").

3. According to its website, Defendant " is the largest bridal and occasion store in America, with 300 locations" across the country.[1]

4. As a condition of receiving products and employment from Defendant, Plaintiff and Class Members were required to entrust Defendant with their sensitive PII, including their names, dates of birth, Social Security numbers, and financial/account information.

5. As the custodian of Plaintiff's and Class Members' PII it collected and maintained, Defendant had a duty to adopt reasonable measures to protect such PII from involuntary disclosure to unauthorized third parties, and to keep it safe and confidential. Defendant had obligations under contract, statutory and common law, industry standards, and representations made to Plaintiff and Class Members to keep their PII secure and to protect it from unauthorized access and disclosure.

6. Defendant breached these duties owed to Plaintiff and Class Members by failing to safeguard the PII that it collected and maintained, including by failing to implement industry standards for data security to protect against cyberattacks, resulting in the Data Breach.

7. As a direct result of the Data Breach, which Defendant failed to take reasonable steps to prevent, the PII of Defendant's customers and employees, including Plaintiff and Class Members, was stolen into the hands of notorious cybercriminals.

8. According to a white paper co-authored by the Cybersecurity & Infrastructure

[1] *See* https://www.davidsbridal.com/stores/pembrokepines-fl-33027-0015.

Security Agency ("CISA"),[2] once LockBit exfiltrates individuals' PII in cyberattacks like this Data Breach, its *modus operandi* is to demand a ransom payment from the affected business. If the ransom payment is not made within a specified time, LockBit publishes the exfiltrated PII to its Dark Web portal.

9. On January 22, 2024, LockBit claimed responsibility for the cyberattack on Defendant, posting some PII it stole from Defendant's systems on its Dark Web extortion portal and declaring it would publish all PII stolen in the Data Breach on January 26 if Defendant did not comply with its ransom demand.

10. Accordingly, based on LockBit's ransom demand to Defendant, Defendant almost certainly knew by January 22, 2024, that the LockBit cyberattack had occurred.

11. Similar to LockBit, the WereWolves ransomware group "is known for its adoption of the 'double extortion' tactic . . . involv[ing] not only demanding a ransom for the decryption of data but also posting sensitive data about non-compliant victim companies on their own Data Leak Site."[3]

12. On February, 2024, WereWolves claimed responsibility for the second cyberattack on Defendant, threatening to publish the PII stolen in the Data Breach if Defendant did not comply with its ransom demand for $850,000.00.

13. Accordingly, based on WereWolves's ransom demand to Defendant, Defendant almost certainly knew by February 14, 2024, that the WereWolves cyberattack had occurred.

14. Upon information and belief, and given that LockBit and WereWolves are

[2] *See* Cybersecurity & Infrastructure Security Agency, *#StopRansomware: LockBit 3.0*, CISA (March 16, 2023), available at https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf (last visited July 26, 2024).

[3] *See* HackManac, Werewolves: A First Analysis of the Russian-Speaking Ransomware Group (2024), available at https://hackmanac.com/news/werewolves-a-first-sight-of-the-russian-ransomware-group (last visited July 26, 2024).

notorious cybercriminal organizations whose *modi operandi* are to publish and sell stolen PII on the internet black market, Plaintiff's and Class Members' PII compromised in the Data Breach has been published and disseminated on the Dark Web.

15. Plaintiff and Class Members now face a lifetime risk of identity theft due to the nature of the PII stolen and now disseminated, which they cannot change and cannot be made private again.

16. To make matters worse, despite that the LockBit cyberattack occurred in January 2024 and the WereWolves cyberattack occurred in February 2024, Defendant to date—*six months* later—has failed to provide any notice or information whatsoever to Plaintiff and Class Members regarding the Data Breach or the fact that their PII is now in two criminal ransomware groups' possessions and almost certainly disseminated on the Dark Web, depriving Plaintiff and Class Members the opportunity to mitigate harm from the Data Breach timely.

17. Defendant's cybersecurity failures, its resultant Data Breach, and its complete lack of adequate or any notice to victims of the Data Breach injured Plaintiff and Class Members in multiple ways, including (i) actual identity theft, and the imminent risk thereof; (ii) the lost or diminished value of their PII; (iii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) out-of-pocket expenses and lost opportunity costs to mitigate the Data Breach's consequences, including lost time; (v) loss of privacy, including through the publication and dissemination of their PII on the Dark Web; (vi) loss of the benefit of their bargain with Defendant; and (vi) emotional distress associated with the loss of control over their highly sensitive PII and attendant, certain risk of identity theft and fraud.

18. Defendant's failure to protect Plaintiff's and Class Members' PII has harmed and

will continue to harm thousands of Defendant's current and former patients and employees, causing Plaintiff to seek relief on a class-wide basis.

19. Plaintiffs bring this action on behalf of herself and all others similarly situated, the proposed Class of persons whose PII was compromised in the Data Breach, asserting causes of action for (I) Negligence/Negligence *Per Se*; (II) Breach of Implied Contract; (III) Breach of Fiduciary Duty; (IV) Violations of the California Consumer Privacy Act, Ca. Civ. Code §§ 1798.100, *et seq.* ("CCPA"); and (V) Unjust Enrichment; seeking an award of monetary damages and injunctive relief, due to Defendant's failure to adequately protect Plaintiff and Class Members' highly sensitive PII and Plaintiff's and Class Members' resulting injuries.

PARTIES

20. Plaintiff is a natural person, resident, and citizen of California. Plaintiff is a former employee and customer of Defendant and, upon information and belief, is and was a victim of Defendant's Data Breach.

21. Defendant David's Bridal, Inc. is a Delaware corporation with its headquarters and principal place of business at 1001 Washington Street, Conshohocken, Pennsylvania 19428. Defendant has thousands of customers and employees located throughout the United States.

JURISDICTION AND VENUE

22. This Court has personal jurisdiction over Defendant because its principal place of business is in Pennsylvania and, personally or through its agents, it engages in substantial and continuous activities in Tennessee and conducts business in this state.

23. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the amount in controversy exceeds $5 million, exclusive of interest and costs, the number of Class Members is over 100, and at least one Class

Member is a citizen of a state that is diverse from Defendant's citizenship, namely, Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law pursuant to 28 U.S.C. § 1367.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant has its principal place of business located in this District, and a substantial part of the events giving rise to this action and Plaintiff's claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

David's Bridal is a Large Corporation That Controls Massive Amounts of Sensitive Data

26. According to David Bridal's website, Defendant "is the largest bridal and occasion store in America, with 300 locations"[4] across the United States and in Canada,[5] serving thousands of customers and employing hundreds of individuals.

27. As a condition of receiving employment and/or products and related services from Defendant, Plaintiff and Class Members were required to entrust Defendant with their sensitive PII including names, addresses, identification documents, dates of birth, Social Security numbers, and financial/account information, and did turn over such PII to Defendant.

28. In exchange for receiving Plaintiff's and Class Members' PII, Defendant promised to safeguard the sensitive, confidential data and only to use it for authorized and legitimate purposes.

29. At all relevant times, Defendant knew it was storing and using its networks to store and transmit Plaintiff's and Class Members' valuable, sensitive PII, and that as a result, its systems would be attractive targets for cybercriminals.

[4] *See* https://www.davidsbridal.com/stores/coralgables-fl-331345403-0073.
[5] *See* https://www.davidsbridal.com/store-list.

30. Defendants also knew that any breach of its network and exposure of the information stored therein would increase the risk of identity theft and fraud for the individuals whose PII was compromised, as well as intrusion into those individuals' highly private financial information.

31. Moreover, the January 2024 cyberattack by LockBit surely should have impressed upon Defendant the need to secure the sensitive PII in its custody. Instead, Defendant did nothing, allowing the WereWolves breach to occur less than one month later.

32. Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII it collected would be kept safe and confidential, the privacy of that information would be maintained, and Defendant would delete any sensitive information after it was no longer required to maintain it.

33. Indeed, Defendant's "Privacy Rights" notice published on its website promises in part as follows:

> Your Privacy and the Security of Your Personal Information is Very Important to Us.
>
> David's Bridal, Inc, a Delaware corporation, and our respective divisions, subsidiaries and affiliates (collectively, "David's Bridal", "we", "us", or "our") are committed to maintaining your confidence and trust. We have adopted the following privacy policy to explain our practices relating to the information we collect, and the information you provide to us, through your completion of a registration or other form in one of our US retail stores, and from your visit to and use of US websites, and other mobile applications, content and services (collectively, the "Service") we make publicly available. This Privacy Policy protects consumers and job candidates providing information through our US websites, US stores or other communication channels[.]
>
> * * *

> **I. How does David's Bridal protect my personal information?**
>
> We take precautions to protect the personal information we collect. We have implemented industry standard and commercially reasonable physical, technological, and administrative procedures to safeguard and secure the personal information we collect.[6]

34. Defendant's Notice of Privacy Practices published on its website further promises and warrants to its customers that the PII Defendant collects from them will only be used or disclosed for specific enumerated reasons, none of which include exposure to criminal ransomware organizations or publication on the Dark Web.[7]

35. Additionally, based on information and belief, Defendant acknowledges the importance of properly safeguarding its employees' PII and promised its employees, including Plaintiff and Class Members, that they would keep their PII safe through reasonable data security measures.

36. Plaintiff and Class Members would not have entrusted their PII to Defendant without its promises to safeguard that information, including in the manners outlined in Defendant's data privacy notices, agreements, and policies.

37. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the operations or services necessary for its business, including employment and payroll functions and retail sales and financing.

38. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff and Class Members, and knew or should have known that it was responsible for protecting their PII from unauthorized disclosure.

---

[6] *See* https://www.davidsbridal.com/legal/privacy-policy.
[7] *See id.*

39. Moreover, Defendant had and has duties to adopt reasonable measures to keep Plaintiff's and Class Members' PII confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of their data management systems and those of its vendors and affiliates. Such duties arise from common law, the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), contract, industry standards, and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain their PII's confidentiality and integrity. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard it.

41. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

42. Plaintiff and Class Members relied on Defendant, as a sophisticated business entity, to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Defendant failed to do so.

David's Bridal Failed to Adequately Safeguard Plaintiff's and Class Members' PII, Which Caused the Data Breach.

43. Defendant collected and maintained its current and former customers' and employees' PII in its computer information technology systems and networks, including when the Data Breach occurred.

44. The information held by Defendant at the time of the Data Breach and compromised therein included the unencrypted PII of Plaintiff and Class Members.

45. On or about January 22, 2024, the notorious ransomware group LockBit accessed Defendant's network systems and exfiltrated Plaintiff's and Class Members' unencrypted PII stored therein.

46. According to its Dark Web post, the files LockBit obtained from Defendant in the Data Breach contained "highly valuable and critical data, encompassing a substantial volume of personal and corporate information."[8]

47. According to a March 2023 whitepaper published by CISA,

> Affiliates deploying LockBit 3.0 ransomware gain initial access to victim networks via remote desktop protocol (RDP) exploitation, drive-by compromise, phishing campaigns, abuse of valid accounts, and exploitation of public-facing applications. . . . After files are encrypted, LockBit 3.0 drops a ransom note with the new filename .README.txt and changes the host's wallpaper and icons to LockBit 3.0 branding.[9]

48. The CISA whitepaper includes the following example of a LockBit ransom note following a cyberattack like this Data Breach[10]:

> ~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~
>
> >>>>> Your data is stolen and encrypted.
>
> If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

49. According to LockBit's Dark Web post, and in line with its *modus operandi* to demand ransom payments from the businesses affected by its cyberattacks and to publish the confidential information it obtains if such payment is not made, LockBit demanded a ransom

---

[8] *See* https://x.com/H4ckManac/status/1749723424010768588/photo/1.

[9] *See See* Cybersecurity & Infrastructure Security Agency, *#StopRansomware: LockBit 3.0*, CISA (March 16, 2023), available at https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf (last visited July 26, 2024).

[10] *See id.*

payment from Defendant following the Data Breach, with a deadline of January 26, 2024.

50. Additionally, given that LockBit is notorious for publishing the PII it steals from companies like Defendant on its Dark Web portal, upon information and belief Plaintiff's and Class Members' PII has almost certainly been published on the Dark Web.

51. Soon after LockBit exfiltrated Plaintiff's and Class Members' from Defendant's systems, the WereWolves criminal ransomware organization followed suit and similarly accessed and obtained Plaintiff's and Class Members' PII from Defendant in another cyberattack, on or about February 14, 2024.

52. According to its Dark Web post, the files WereWolves obtained from Defendant in the Data Breach contained "very valuable and important data covering a significant amount of personal and corporate information."

53. According to reporting on the WereWolves cyberattack, WereWolves's strategy

> involves double extortion tactics, whereby they not only encrypt the victim's data but also threaten to publicly release it unless a ransom is paid. . . . The group's targeting approach is diverse, affecting a broad spectrum of industries and businesses worldwide. As of January 2024, they have targeted 23 victims, primarily mid to small-scale enterprises and organizations, indicating a preference for easier targets. . . . Originating from Russian-speaking backgrounds, the WereWolves ransomware group has targeted sectors ranging from finance to manufacturing. Although their approach seems random, they appear to focus on easily penetrable yet high-impact industries like small to mid-scale services and organizations.[11]

54. According to WereWolves's Dark Web post, and in line with its *modus operandi* to demand ransom payments from the businesses affected by its cyberattacks and to publish the confidential information it obtains if such payment is not made, WereWolves demanded a

[11] *See* Halycon AI, *WereWolves attack David's Bridal* (Feb. 2024), available at https://ransomwareattacks.halcyon.ai/attacks/werewolves-attacks-davids-bridal (last visited July 26, 2024).

$850,000.00 ransom payment from Defendant following its Data Breach.

55. Additionally, given that WereWolves is notorious for publishing the PII it steals from companies like Defendant on its Dark Web portal, upon information and belief Plaintiff's and Class Members' PII has almost certainly been published on the Dark Web.

56. Defendant was certainly on notice of the importance of guarding against a possible attack from cybercriminals like WereWolves given that it had just experienced a similar cyberattack the previous month.

57. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach. The LockBit and WereWolves hackers accessed and acquired files stored without reasonable security on Defendant's systems and containing Plaintiff's and Class Members' unencrypted PII.

58. Defendant did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiff's and Class Members' PII that it collected and maintained, such as encrypting the information or deleting it when it was no longer needed, which caused the theft of that PII in the Data Breach

59. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class Members' PII and training its employees on standard cybersecurity practices, but failed to do so.

60. For example, if Defendant had implemented industry-standard logging, monitoring, and alerting systems—basic technical safeguards that any PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate at least three days of malicious activity in Defendant's information system without alarm bells going off, including the reconnaissance necessary to identify where Defendant stored PII, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data,

staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

61. Defendant would have recognized the activities detailed in the preceding paragraph if it had bothered to implement basic monitoring and detection systems, which would have stopped the attack or significantly reduced its impact.

62. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' PII, meaning Defendant had no effective means in place to detect and prevent attempted cyberattacks.

63. As a result of Defendant's failures, Plaintiff's and Class Members' PII was stolen in the Data Breach when two criminal hacker groups accessed and acquired files in Defendant's computer systems containing that sensitive PII in unencrypted form.

64. To make matters worse, Defendant has yet to provide any warning, notice, or information whatsoever to Plaintiff, Class Members, or the public that the Data Breach occurred, let alone relevant details about the Data Breach like the extent of PII compromised or that such PII was accessed by two notorious Russian ransomware organizations, which have now published it on the Dark Web.

65. Defendant's deficient and, indeed, non-existent notice exacerbated Plaintiff's and Class Members' injuries and caused additional damages by depriving them of the opportunity to mitigate harm from the Data Breach in a timely manner.

66. Moreover, in the aftermath of the Data Breach, Defendant has not indicated any measures it has taken to mitigate the harm or prevent future breaches of its systems or whether it has remedied the deficiencies that resulted from the Data Breach. Nor has Defendant offered

affected individuals any redress or compensation for harm the Data Breach has caused or will cause them.

David's Bridal Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses like Defendant in Possession of PII are Particularly Suspectable.

67. Defendant's negligence, including its gross negligence, in failing to safeguard Plaintiff's and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

68. PII of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for various unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the Dark web.

69. PII can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone or in combination with other personal or identifying information connected or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

70. Data thieves regularly target businesses like Defendant due to the highly sensitive information they maintain. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminals who seek to monetize it through unauthorized access illegally.

71. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[12]

[12] Tom Kellermann, *Cyber Bank Heists: Threats to the financial sector*, at 5, CONTRAST SECURITY https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf (last accessed July 8, 2024).

72. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable retailer and employer, should have known that the PII it collected and maintained would be targeted by cybercriminals.

73. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[13]

74. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and anyone in Defendant's industry, including Defendant itself. "For 83% of companies, it's not if a data breach will happen, but when."[14]

75. Defendant was on specific notice that it should guard against a possible LockBit attack like this Data Breach. In its June 2023 whitepaper, CISA described that, as of 2022, LockBit was the most deployed ransomware variant worldwide, attacking organizations across an array of critical infrastructure sectors including healthcare. Between January 2020, when LockBit was first deployed, approximately $91 million in ransom has been paid to LockBit by United

[13] *See* Identity Theft Resource Center, *2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[14] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach (last accessed July 8, 2024).

States organizations.[15]

76. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

77. As a sophisticated business entity in possession of its customers' and employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members because of their PII's unauthorized exposure to bad actors. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

78. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' PII compromised therein would be targeted by hackers and cybercriminals, including LockBit specifically, for use in various injurious ways. Indeed, cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

79. Defendant was or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to thousands of individuals' detailed PII, and, thus, the significant number of individuals whom the exposure of the unencrypted data would harm.

80. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have

[15] Cybersecurity & Infrastructure Security Agency, *Understanding Ransomware Threat Actors: LockBit — Alert Code: AA23-165A*, CISA (June 14, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.

known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

81. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

82. Moreover, the Defendant's previous data breach put the Defendant on notice of the importance of meeting its obligations under statute, regulation, and common law, as well as the types of harms associated with such data breaches.[16]

David's Bridal is Required but Failed to Comply with FTC Rules and Guidance.

83. The FTC has promulgated numerous business guides highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

84. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17]

85. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

[16] *Statement Regarding Theft and Data Breach at the Tacoma, WA Office*, NUMOTION, https://www.numotion.com/about-us/news/statement-regarding-theft-and-data-breach-at-the-t (last visited July 8, 2024).

[17] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).

someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

86. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

87. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders from these actions further clarify the measures businesses like Defendant must undertake to meet their data security obligations.

88. Such FTC enforcement actions include actions against healthcare entities like Defendant. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

89. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above form part of the basis of Defendant's duty in this regard.

[18] *Id.*

90. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[19]

91. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

92. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

David's Bridal Failed to Comply with Basic Industry Standards.

93. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

94. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software

[19] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

Security, Incident Response Management, and Penetration Testing.[20]

95. The NIST also recommends certain practices to safeguard systems, such as the following:

> a. Control who logs on to your network and uses your computers and other devices.
>
> b. Use security software to protect data.
>
> c. Encrypt sensitive data, at rest and in transit.
>
> d. Conduct regular backups of data.
>
> e. Update security software regularly, automating those updates if possible.
>
> f. Have formal policies for safely disposing of electronic files and old devices.
>
> g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[21]

96. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other

---

[20] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

[21] Federal Trade Commission, *Understanding the NIST Cybersecurity Framework*, FTC.GOV, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last accessed July 8, 2024).

steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs."[22]

97. Upon information and belief, Defendant failed to implement industry- standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and Class Members' PII, resulting in the Data Breach.

As a Major Corporation, David's Bridal Owed Plaintiff and Class Members a Common Law Duty to Safeguard their PII.

98. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and

[22] Cybersecurity & Infrastructure Security Agency, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed July 8, 2024).

protocols adequately protected Plaintiff's and Class Members' PII.

99. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to protect PII adequately.

100. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner.

101. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

102. Defendant owed a duty to Plaintiff and Class Members to promptly and accurately disclose when and how the Data Breach occurred.

103. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

104. Defendant tortiously failed to take the precautions required to safeguard and protect Plaintiff's and Class Members' PII from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

Plaintiff and Class Members Suffered Damages Because of the Data Breach

105. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' PII directly and proximately caused injuries to Plaintiff and Class Members by the consequential disclosure of their PII to cybercriminals in the Data Breach.

106. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to (a) closely monitor their medical

statements, bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

107. The unencrypted PII of Plaintiff and Class Members compromised in the Data Breach has *already* been published on the Dark Web, including photocopied images of Data Breach victims' employment applications, payment forms, and tax documents with data like full names, addresses, Social Security numbers, and financial information. Unauthorized individuals with nefarious intentions can now easily access Plaintiff's and Class Members' PII—and have likely done so already.

108. The ramifications of Defendant's failure to secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

109. Once PII is exposed, virtually no way exists to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct which caused the Data Breach. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

110. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of PII.

111. A recent study found that 28% of consumers affected by a data breach become victims of identity fraud, a significant increase from a 2012 study that found that only 9.5% of

those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[23]

112. The reality is that cybercriminals seek nefarious outcomes from a data breach" and stolen data "can be used to carry out a variety of crimes."[24]

113. Plaintiff and Class Members are also at a continued risk because their PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack on multiple occasions and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its employees' and customers' PII.

Plaintiff's Experience as a Former Customer and Employee of David's Bridal

114. Plaintiff is a former customer and employee of Defendant. She was required to provide Defendant with her PII to obtain employment and products from Defendant.

115. At the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

116. Upon information and belief, the stolen PII comprised Plaintiff's name, date of birth, address, Social Security information, and financial/account information.

117. Plaintiff is very careful about sharing her sensitive PII. She stores documents containing her PII in a safe and secure location and has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source.

118. As a result of the Data Breach perpetrated by notorious cybercriminals, Plaintiff has spent considerable time and effort attempting to remediate the harmful effects of the Data Breach, including seeking legal advice in response to the Data Breach, and to prevent fraudulent

[23] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last accessed July 8, 2024).
[24] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

misuse or damages, as well as time and effort to monitor her accounts to protect herself from additional identity theft. Plaintiff's lost time is a monetary injury.

119. Plaintiff fears that her personal financial security is at substantial risk and because of the uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, stress, and fear because of the Data Breach, which goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim the law provides redress for.

120. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach. This has been compounded by Defendant's failure to notify Plaintiff of the Data Breach. Plaintiff has had to expend the above time and effort to rectify the impacts of the Data Breach and does not know how many more attempts may arise for her lifetime.

121. As a result of Defendant's inadequate data security practices and the resulting Data Breach, Plaintiff faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like her Social Security number

122. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including expending time to check her bills and accounts to make sure they were correct, which time she would not have been required to spend on such tasks but for the Data Breach. Plaintiff has spent significant time dealing with the Data Breach, which she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever, cannot be recaptured, and is a monetary injury that has already occurred.

123. Plaintiff additionally anticipates spending considerable time and money on an

ongoing basis to address the injuries and harms caused by the Data Breach.

124. As a result of the Data Breach, Plaintiff is presently and imminently at risk and will continue to be at such increased risk of identity theft and fraud for years to come.

125. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future cyberattacks.

PLAINTIFF AND CLASS MEMBERS SUFFERED COMMON INJURIES AND DAMAGES

126. As the direct and proximate result of Defendant's ineffective and inadequate data security practices and the resulting Data Breach, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

127. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including but not limited to (a) invasion of privacy; (b) out of pocket costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) out of pocket costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of the benefit of the bargain (price premium damages); (h) diminution of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake adequate measures to protect it.

The Risk of Identity Theft to Plaintiff and Class Members Is Present and Ongoing.

128. The link between a data breach and identity theft risk is simple and well

established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit various identity theft-related crimes discussed below.

129. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

130. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

131. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[25] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[26] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

132. A sophisticated black market exists on the dark web where criminals can buy or

[25] Louis DeNicola, *What Is the Dark Web?*, EXPERIAN (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web.
[26] *Id.*

sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here. The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information. As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[27]

133. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[28]

134. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the

[27] *What is the Dark Web?*, MICROSOFT 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[28] Social Security Administration, *Identity Theft and Your Social Security Number*, SSA.GOV (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

135. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[29]

136. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[30]

137. One such example of criminals using PII for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

138. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included

[29] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[30] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as identity thieves or illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and Class Members' stolen PII is being misused, and that such misuse is traceable to the Data Breach.

139. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[31]

140. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[32] Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

141. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

142. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

[31] *See 2019 Internet Crime Report Released* (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[32] *Id.*

143. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized use of their PII for years to come.

Plaintiff and Class Members Lost Time Mitigating the Risk of Identify Theft and Fraud

144. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual learns his or her PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm–yet the asset of time has been lost.

145. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

146. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[33] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if

[33] *See* U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[34]

Plaintiff and Class Members Suffered Diminution of Value of their PII

147. PII is a valuable property right.[35] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

148. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

149. PII can sell for as much as $363 per record according to the Infosec Institute.[36]

150. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data sells on the dark web for $50 and up.[37]

151. An active and robust legitimate marketplace for PII also exists. In 2019, the data

[34] *See* Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed July 8, 2024).
[35] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[36] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[37] *Ransomware attacks paralyze, and sometimes crush, hospitals*, SOPHOS NEWS (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals

brokering industry was worth roughly $200 billion.[38] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[39] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[40]

152. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized release onto the Dark Web, where it is now available for additional criminals to access and holds significant value for the threat actors.

Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary.

153. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach.

154. LockBit and WereWolves have already published PII exfiltrated in the Data Breach on the Dark Web. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been or will be further disseminated on the black market/Dark Web for sale and purchase by bad actors intending to utilize the PII for identity theft crimes (e.g., opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims).

155. Such fraud may go undetected until debt collection calls commence months, or

[38] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak* (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[39] https://datacoup.com/.
[40] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

156. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[41] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers and birth certificate photocopies).

157. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

158. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss of Benefit of the Bargain

159. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

160. When agreeing to provide their PII, which was a condition precedent to obtaining products and related services from Defendant, and paying Defendant, directly or indirectly, for its products and services, Plaintiff and Class Members, as Defendant's customers and consumers,

[41] *See* Jesse Damiani, *Your Social Security Number Costs $4 On the Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

understood and expected that they were, in part, paying for services and data security to protect the PII they were required to provide.

161. When agreeing to provide their PII, which was a condition precedent to obtain employment and compensation from Defendant, Plaintiff and Class Members, as current and former employees, understood and expected they were being compensated, in part, commensurate with Defendant's data security to protect the PII they were required to provide.

162. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

Lack of Compensation

163. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their PII in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

164. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of fraud and identity theft.

165. Further, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

166. Specifically, victims suffered and will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the

effects of the Data Breach relating to

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying fees for late or declined payments fees imposed for failed automatic payments tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

167. In addition, Plaintiff and Class Members suffered a loss of value of their PII when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

168. Plaintiff and Class Members are forced to live with the anxiety that their PII — which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

Injunctive Relief is Necessary to Protect Against Future Data Breaches.

169. Moreover, Plaintiff and Class Members have an interest in ensuring that PII, which is believed to remain in Defendant's possession, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to employee training on cybersecurity awareness and prevention measures, storing data or documents containing PII so they are not accessible online, and ensuring that access to such data is password-protected.

170. Because of Defendant's failure to use reasonable measures to prevent or detect the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they suffered or are at a materially increased risk of imminently suffering

a. loss of control over how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. unauthorized use of their stolen PII; and

g. continued risk to their PII, which remains in Defendant's possession and is thus at risk for futures breaches so long as Defendant fails to take appropriate measures to protect it.

CLASS ALLEGATIONS

171. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23(a) and 23(b)(3).

172. Plaintiff proposes the following nationwide Class definition, subject to amendment based on information obtained through discovery:

> All individuals whose PII may have been accessed and/or acquired in Defendant's Data Breach beginning on or about January 22, 2024 ("Nationwide Class").

173. Additionally, Plaintiff proposes the following California subclass, pursuant to Federal Rule of Civil Procedure 23(c)(5):

> All residents of California whose PII may have been accessed and/or acquired in Defendant's Data Breach beginning on or about January 22, 2024 ("California Subclass") (Nationwide Class and California Class collectively, "Class").

174. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

175. The "Class" of individuals includes Defendant's former employees and customers. As both a former employee and former customer, Plaintiff has standing to represent the Class or any subclass determined by Court Order. Moreover, Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

176. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

177. This action satisfies the requirements for a class action under Rule 23(a)(1)-(3)

and Rule 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

178. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the PII of approximately 4,190 customers and/or employees of Defendant was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

179. **Commonality, Fed. R. Civ. P. 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether hackers obtained Plaintiff's and Class Members' PII in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

h. Whether Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and Class Members; and

i. Whether Defendant violated the CCPA;

j. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

180. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

181. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating data breach class actions.

182. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' PII was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

183. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all

other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions.

b. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

c. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

d. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

184. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Defendant's employees, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

185. In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, and injunctive relief are appropriate on a class-wide basis. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to give timely or adequate notice of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard customers' and employees' PII; and

f. Whether adherence to FTC data security recommendations, and those by data security experts, would have reasonably prevented the Data Breach.

186. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE/NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

187. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 186 above as if fully set forth herein.

188. Defendant required Plaintiff and Class Members to submit private, confidential PII to Defendant as a condition of receiving products and services and/or employment from Defendant.

189. Plaintiff and Class Members provided certain PII to Defendant including their names, Social Security numbers, dates of birth, addresses, financial information, and other personal information.

190. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that PII.

191. Plaintiff and Class Members were the foreseeable victims of inadequate safety and security practices by Defendant.

192. Plaintiff and the Class Members had no ability to protect their PII in Defendant's possession.

193. By collecting and storing Plaintiff's and Class Members' PII in its computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard

information, prevent disclosure of the information, and safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

194. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

195. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its customers and/or its employees, which is recognized by laws and regulations including but not limited to the FTC Act and common law. Defendant was able to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach, yet it failed to.

196. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

197. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq.*, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

198. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

199. The injuries to Plaintiff and Class Members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of FTC Act.

200. Plaintiff and Class Members are within the class of persons the FTC Act was intended to protect.

201. The type of harm that resulted from the Data Breach was the type of harm the FTC Act was intended to guard against.

202. Defendant's failure to comply with the FTC Act constitutes negligence *per se.*

203. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' confidential PII in its possession arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to reasonably protect such PII.

204. Defendant breached its duties, and was grossly negligent, by acts of omission or commission, by failing to use reasonable measures and indeed even minimally reasonable measures, to protect the Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' PII;

f. Failing to timely notify Plaintiff and Class Members about the

Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

205. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised and their injuries would have been avoided and/or lessened, because Defendant would have identified the malicious activity and stopped the attack before the malicious actors had a chance to inventory Defendant's digital assets, stage them, and then exfiltrate them.

206. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

207. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would cause them to suffer one or more types of injuries.

208. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their PII; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their PII, which remains (i) unencrypted and available for unauthorized third parties to access and abuse; and (ii) in Defendant's possession subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

209. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-

economic losses.

210. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

211. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

212. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 186 above as if fully set forth herein.

213. Defendant required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining products and services and/or employment from Defendant.

214. When Plaintiff and Class Members provided their PII to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such PII and to timely and accurately notify Plaintiff and Class Members if and when their PII was breached and compromised.

215. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their PII to Defendant.

216. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promise to protect PII it collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures. Plaintiff and Class Members provided this PII in reliance on Defendant's promise.

217. Under the implied contracts, Defendant promised and was obligated to (a) provide products and/or employment to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' PII (i) provided to obtain such services and employment and/or (ii) created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide Defendant labor and/or payment and their PII.

218. Both the provision of payment and/or labor, and the protection of Plaintiff's and Class Members' PII, were material aspects of these implied contracts with Defendant.

219. Defendant's implied contracts for data security—that include the obligations to maintain the privacy of Plaintiff's and Class Members' PII—are also acknowledged, memorialized, and embodied in multiple documents, including Defendant's Privacy Practices notices as described *supra*.

220. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

221. In entering into such implied contracts with Defendant, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

222. Plaintiff and Class Members who partnered or contracted with Defendant for products and services and/or employment and who provided their PII to Defendant, reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII. Defendant failed to do so.

223. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their PII to Defendant and agreed Defendant would receive labor and/or

payment for, amongst other things, the protection of their PII.

224. Plaintiff and Class Members performed their obligations under the contracts when they provided their labor and/or payment and PII to Defendant.

225. Defendant materially breached its contractual obligations to protect the PII it required Plaintiff and Class Members to provide when it failed to implement even minimally reasonable logging and monitoring systems, among other safeguards, thus causing the disclosure of Plaintiff's and Class Members' PII to criminals bent on identity theft, fraud, and extortion.

226. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiff and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

227. Defendant materially breached the terms of its implied contracts, including, but not limited to, by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act, or by failing to otherwise protect Plaintiff's and Class Members' PII, as set forth *supra*.

228. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff and Class Members.

229. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and instead received products and services and/or compensation for employment of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the products, services, and/or employment with reasonable data security protection they bargained

for and that which they received.

230. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of the implied contracts between them and Defendant.

231. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have provided their PII under contracts with Defendant.

232. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely, adequate, or any notice that their PII was compromised in and because of the Data Breach.

233. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

234. Plaintiff and Class Members, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

235. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

236. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 186 above

as if fully set forth herein.

237. A fiduciary relationship existed between Plaintiff and Class Members and Defendant in which Plaintiff and Class Members entrusted Defendant to protect their PII. Defendant accepted this trust when it received Plaintiff and the Class Members' PII.

238. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and refrain from disclosing their PII to unauthorized third parties.

239. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII involved an unreasonable risk of harm to Plaintiff and Class Members, including harm that foreseeably could occur through the criminal acts of third parties.

240. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such PII from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and Class Members' PII in Defendant's possession was adequately secured and protected.

241. Defendant also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and Class Members' PII. Defendant's fiduciary duty to use reasonable security measures arose from the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Defendant was entrusted with Plaintiff and Class Members' PII.

242. Defendant breached its fiduciary duty that it owed Plaintiff and Class Members by failing to case in good faith, fairness, and honesty; by failing to act with the highest and finest

loyalty; and by failing to protect the PII of Plaintiff and Class Members.

243. But for Defendant's breach of fiduciary duty, the Data Breach and attendant damages to Plaintiff and Class Members would not have occurred.

244. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class suffered damages have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

245. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

246. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
CALIFORNIA CONSUMER PRIVACY ACT
Ca. Civ. Code §§ 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiff and the California Subclass)

247. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 186 above as if fully set forth herein.

248. At all relevant times, Defendant has done business in the State of California.

249. The CCPA imposes a duty on entities doing business in California to implement and maintain reasonably security procedures and practices as appropriate given the nature of the sensitive information. Ca. Civ. Code § 1798.100.

250. Under the CCPA, "[a] business that, acting as a third party, controls the collection of personal information about a consumer" must inform the customer of (i) the

information being collected, (ii) the purpose for collecting the information and if that information is to be shared or sold, and (iii) the companies' retention policies. *Id.* at (a).

251. The CCPA requires that a business's collection, use, retention, and sharing of a consumer's personal information be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes. *Id.* at (b).

252. Pursuant to CCPA, any individual whose nonencrypted and nonredacted personal information is accessed, exfiltrated, stolen, or disclosed as a result of the business's violation of their duty are entitled to damages, including statutory damages. *Id.* at § 1798.150.

253. Defendant collected Plaintiff's and California Subclass Members' PII on with the purpose of providing products and/or employment in the course and as part of its business in California.

254. Defendant failed to implement reasonable security measures as reasonably necessary and proportionate to the PII it held, in violation of the CCPA.

255. Pursuant to Ca. Civ. Code § 1798.150(b), Plaintiff will send Defendant notice of her CCPA claims shortly after the date of this filing. If Defendant does not correct its business practices, Plaintiff will amend (or seek leave to amend) the complaint to add claims for monetary relief, including statutory and actual damages under the CCPA. To date, Defendant has failed to cure the CCPA violation.

256. As a result of Defendant's CCPA violation, Plaintiff and the California Subclass are entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and

procedures; and (c) provide adequate credit monitoring to all Class Members.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

257. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 186 above as if fully set forth herein.

258. This claim is pleaded in the alternative to the claim of breach of implied contract.

259. Plaintiff and Class Members conferred direct benefits upon Defendant in the form of agreeing to provide their PII to Defendant, without which Defendant could not perform the services it provides or pay its employees.

260. Defendant appreciated or knew of these benefits it received from Plaintiff and Class Members. Under principles of equity and good conscience, Defendant should not be allowed to retain the full value of these benefits—specifically, the costs it saved by failing to implement reasonable or adequate data security practices with respect to the PII it collected from Plaintiff and Class Members.

261. After all, Defendant failed to adequately protect Plaintiff's and Class Members' PII. And if such inadequacies were known, then Plaintiff and Class Members would never have agreed to provide their PII, or payment or labor, to Defendant.

262. Defendant should be compelled to disgorge into a common fund, for the benefit of Plaintiff and the Class, all funds that were unlawfully or inequitably gained despite Defendant's misconduct and the resulting Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law,

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Any and all such relief to which Plaintiff and the Class are entitled.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all issues so triable.

Dated: July 27, 2024

Respectfully submitted,

LAUKAITIS LAW LLC

/s/ Kevin Laukaitis
Kevin Laukaitis (PA Bar #321670)
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Phone: (215) 789-4462
Email: klaukaitis@laukaitislaw.com

Attorneys for Plaintiff and the Proposed Class